The U.S. House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on SCADA Security

March 30, 2004

Statement Submitted for the Record
By
Jeffrey Katz, Chair, Public Policy Division
United Telecom Council

INTRODUCTION

The United Telecom Council - UTC - is the telecommunications and information technology association that represents the interests of America's critical infrastructure entities. UTC and its association partners, the American Gas Association, the American Public Power Association, the Association of American Railroads, the Edison Electric Institute, the National Association of Water Companies, the American Petroleum Institute, the American Water Works Association, the Association of Oil Pipe Lines, the Interstate Natural Gas Association, and the National Rural Electric Cooperative Association, represent virtually every electric, gas and water utility and every communications network used to operate, control and maintain our nation's critical infrastructure (CI).

Some of us, at least, may remember a time when Americans could tolerate interruptions to the delivery of the critical infrastructure services delivered to them, such as electric power, natural gas, steam and water. Commerce and government continued to operate because paper and pencil recordkeeping was all anyone needed. Public safety agencies continued to operate because they used older telephone equipment that needed no external electric power. If their voice two-way radio system failed they could station patrol units at pole-mounted call boxes as a fallback. Things are very different today.

Today the very fabric of our nation depends upon the reliability and availability of services provided by America's critical infrastructure ('CI') industries. Every federal building, every military base, every railroad, every mass transit system, every telephone central office, every cell site, every traffic signal, every toll booth, every school, college and university, every hospital, every bank, every stock and commodity exchange depends upon an available and reliable supply of electric energy. Many also depend upon natural gas and water. If electric power fails, water service also can fail because water utilities use electric pumps to distribute water to consumers. Fire suppression

efforts are impacted if hydrant service cannot be maintained. If electric power fails, central heating unit furnace blowers or boiler circulators cannot operate.

The services provided by CI no longer are mere conveniences whose loss we can tolerate. They are necessary for the health, safety and welfare of our nation and our people. Congress recognized this in the Balanced Budget Act of 1997 (P.L. 105-33) by determining that CI is a 'public safety radio service' under the provisions of the Communications Act of 1934 (47 U.S.C. 309 (j)(2) and FCC 00-403). Congress again acknowledged the importance of CI as a critical component of our nation's well being in Section 1016 of the USAPATRIOT Act.

Every CI entity depends upon telecommunications systems for SCADA, telemetry, command & control, remote actuation, and protective relaying operations. In addition, for both routine communications and during disasters and outages, CI entities depend upon private internal data and voice networks to direct the workforce and to restore service. To the extent that private internal communications systems are not available, reliable and exclusive, outages are extended; restoration is delayed; worker and public safety are compromised. In its January 2002 report on the current and future use of spectrum by the energy, water, and railroad industries, the National Telecommunications and Information Administration (NTIA) within the US Department of Commerce, recognized the importance of these systems in stating that, "the significance of these industries and the urgency of these issues [concerning spectrum use] may have changed as a result of the September 11th events. . . . . [I]t is of the utmost importance that the Federal Communications Commission revisit these critical [spectrum use] issues in order to accommodate the increasing role these industries play in maintaining quality of life."

POLICY ISSUES THAT NEED TO BE ADDRESSED

The overriding Issue that CI and Congress must address is: What federal or state policies, laws or regulations impact negatively CI's ability to avoid service interruptions, to reduce the duration and scope of service interruptions and to make CI, including its SCADA systems, less vulnerable to attack by non-physical intrusion? In many cases, these policies, laws or regulations actually run counter to homeland security objectives.

- **Public access to sensitive radio frequency information provides data useful to those who would do us harm. The federal system of record, the FCC's Universal Licensing System, is accessible by the general public via the internet. (47 CFR Sec 1.911).**

The FCC's Universal Licensing System (www.fcc.gov/wtb/uls) allows access to technical and location data regarding any FCC licensee. Anyone who would do us

harm will find all they need courtesy of the FCC. It is time for the federal government not to be a willing partner in advertising vulnerabilities.

CI wireless SCADA, telemetry, command & control, data and voice systems can be compromised with the information contained within the FCC's public databases. A method must be found to make this information less public, either through creation of a confidential licensing category, or by providing the FCC with other authority, such as that enjoyed by NTIA, to exercise discretion concerning mission-critical telecommunication systems data. To that end, UTC urges greater flexibility be offered NTIA and the FCC in managing Federal and non-Federal spectrum use data, including providing NTIA with more flexibility for appropriate spectrum sharing with non-federal entities and thereby allowing greater confidentiality of licensing data.

- **Infrastructure data is made unnecessarily public through the FCC's pole attachment regulations and other provisions of the Telecommunications Act.**

Pursuant to the Telecommunications Act of 1996, maps of utility infrastructure must be made available to potential attachers upon the most minimal of showings, and those interested in attaching fiber-optic cable or other equipment to utility infrastructure are permitted to employ third-party contractors rather than personnel trained to observe strict safety regulations. Utilities are under significant pressure from the FCC to relax safety standards observed across the industry (the National Electric Safety Code, or NESC) for the purposes of telecommunications attachments to electric infrastructure. Indeed, language in a recent FCC attachment complaint decision dismissed a utility's concerns about the continued safety of its own infrastructure based on the lack of any serious accidents or harm thus far. One must wonder what the FCC is waiting to see happen before its attitude toward critical infrastructure protection changes.

- **Significant investment in better and more secure communications systems is hampered because such investments often are not immediately recoverable in rates and because the spectrum in which SCADA systems operate is not exclusive**.

Regulated entities are not able to recover capital investments through rate relief without filing a 'rate case' with state regulators. Rate cases are time consuming, tedious, and must be filed in each state in which the utility serves consumers. Further complicating the situation is the fact that most of our nation's utilities have a multi-state presence that would require consistent cost recovery schemes between and among the states.

Utility SCADA, telemetry, command & control, data and voice systems are system-wide, not statewide. Prudent and necessary investments in enhanced security, reliability and functionality should be recoverable immediately in rates, without the need to file a rate case in each state, and the specifics of the investment should be privileged and classified.

At the same time, why should private wireless SCADA systems be upgraded if the asset becomes stranded, due either to changes in the FCC regulatory environment or the possibility of co-channel or adjacent-channel interference? In many instances, utilities have been forced to operate wireless-based SCADA systems on bands where they have secondary status and may actually be required to shut down operations under FCC rules. Or they must operate these critical systems on bands shared with non-CI entities with little respect for FCC rules, creating interference and affecting reliability. This lack of spectrum exclusive to CI also serves as a disincentive to investment.

- **State and local governments should receive guidance from the Federal government as to the reasonable measures they can expect from industry.**

CI should be encouraged to adopt by a date certain voluntary industry standards (best practices) for telecommunications security. If such standards are not so adopted, then and only then, should standards be mandated by statute or by regulation**.**

UTC does not advocate that additional mandates be imposed on CI industries to ensure SCADA and/or telecommunications system security. This panel has heard my colleagues' testimony about efforts already underway and ongoing, and the ideal role of the Federal government in providing the small amount of funding needed to continue the work of the national laboratories and test beds. However, in an area as complex and large-scale as Homeland Security, state and local governments and regulators look to the Federal government for some guidance on the reasonable measures they can expect from industry. CI entities that invest in security measures meeting previously defined guidelines, should expect to win cost recovery approval from state regulators. Moreover, federal guidance would facilitate investments not only by large investor-owned utilities, but also by small municipals and cooperatives, all of which are faced with severe budget constraints and are under constant pressure to control rates.

A mandate would be even more likely to ensure cost recovery approval; however, the inevitable unevenness of applying government mandates among smaller entities, such as municipal utilities, co-ops and water systems, along with larger, multi-state entities, makes this solution undesirable.

- **Some federal agencies, including the FCC, erroneously believe that the communication needs of CI can be met by the use of Commercial Wireless Service ('CWS') providers such as cellular and personal communications services ('PCS').**

CI must work during times when utility services are likely not to be available, and their communications systems must withstand outages and storm damage. This is why CI entities build, own and operate their own private internal communications systems for

SCADA, telemetry, date, voice, and command/control of utility plant. And CI builds these systems so that they remain in operation for weeks under the worst conditions.

CWS providers, including cellular and PCS, generally have limited duration battery backup and are not designed to be continuously available or 100% reliable or exclusive. CWS does not provide ubiquitous coverage throughout a CI entity's operating territory. CWS builds its infrastructure where the revenue and subscribers are. CWS services are among the first to fail during a widespread power outage and, if they do not fail, they quickly become saturated as affected persons place calls or receive calls. CWS internal network latencies, which change over time and by subscriber link, prevent critical orders from being acted upon at precisely the same time by several different people at different locations.

August 14, 2003 probably is the most recent CI event. First, it is important to note that most if not all SCADA systems, including protective relaying, operated as designed. These systems protected automatically generation, transmission, switching station and substation assets from the effects of cascading outages and overloads. Second, while these systems automatically shut down utility plant in service, they are not designed to restore service after a blackout of such magnitude. Service restoration from cold start requires a carefully choreographed process involving hundreds of personnel at dozens of locations all performing specific tasks at precisely the right time. Coordination of that process and those players requires a voice communications system that is available to each of them and that does not have asymmetric network latencies. Utilities involved relied exclusively on their private internal systems. CWS had failed or operating cell sites were saturated. Wired telephone service was not available at each location. Cellular service, even if working, was not available at each location and the network latencies inherent in cellular systems was not conducive to the simultaneous execution of instructions.

Moreover, reliance on the "Wireless Priority Access System" (WPAS) is misplaced. WPAS does not afford CI the same availability, reliability and exclusivity as private wireless systems. First, WPAS must be applied for via rule waiver by a CWS provider under 47 C.F.R. Sec. 64.402 App. B. Second, WPAS has a hierarchy of access rights, with CI being 4th out of 5. Third, WPAS does not mean 'ruthless preemption'. Calls in progress are not interrupted. All WPAS does is bump a higher priority caller ahead of a lower priority caller in waiting for access. Fourth, CWS is among the first to fail in situations when CI needs communications most. and, since WPAS is CWS based, WPAS has no value. Fifth, WPAS anticipates normal cellular usage, it is not designed to handle 'dispatch' operations where instructions are issued that must be heard simultaneously by many people. WPAS offers nothing in the way of availability, reliability, and exclusivity.

In conclusion, UTC appreciates the opportunity to provide this statement to the Subcommittee. We would be pleased to provide any additional material that the Subcommittee may require for its deliberations.